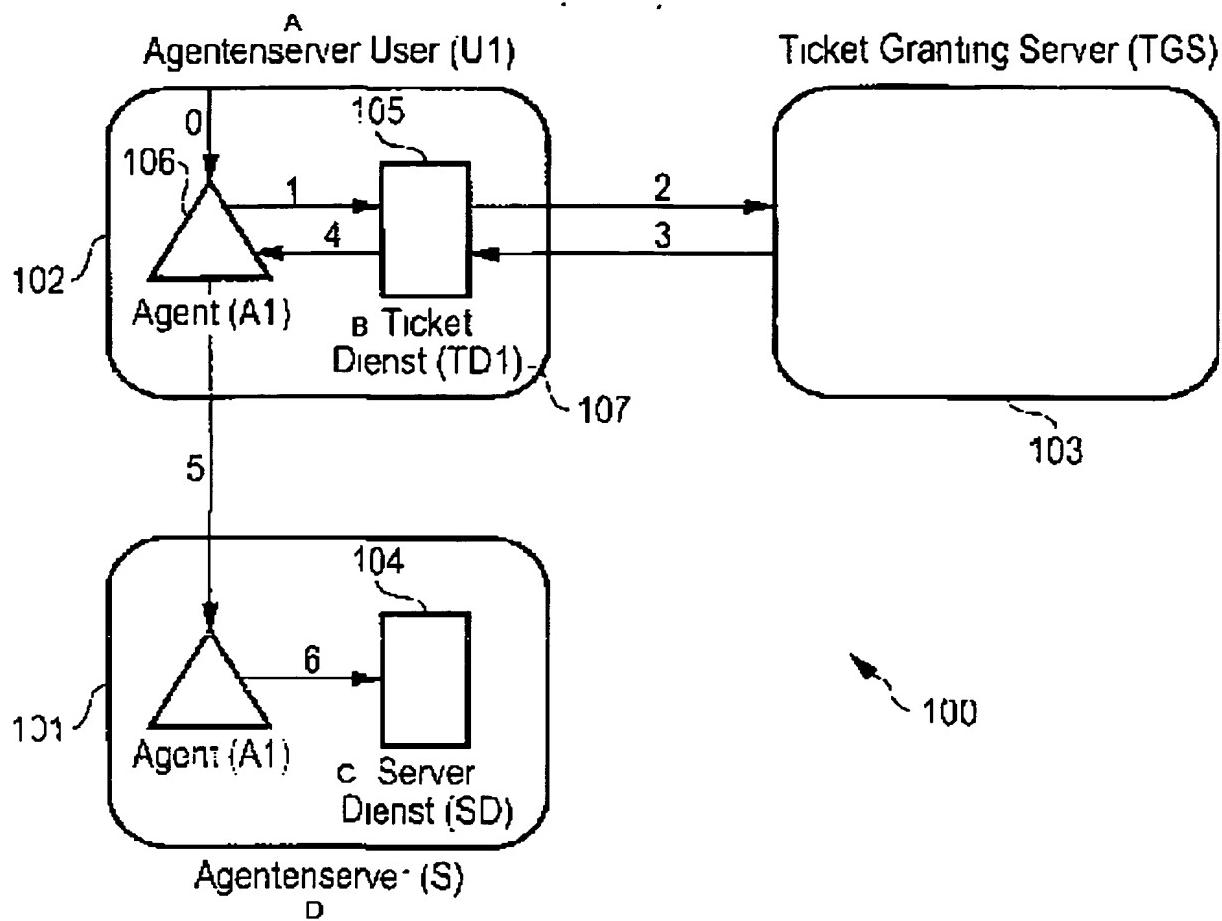


AN: PAT 2003-833818
TI: Mobile agent authorization method for use in a communications network, whereby an authorization authority processes an authorization request and generates authorization data so that the agent can access a service
PN: WO2003088012-A1
PD: 23.10.2003
AB: NOVELTY - Method for authorization of a mobile agent in a communications network to access a service offered in the communications network, where the agent is an independent, autonomous computer program used to access said service. An authorization request is made to an authorization authority in the communications network, which authorizes access of the mobile agent to the service. The request is verified by the authority, which generates authorization data accordingly. The data is furnished to the agent to allow it to access the service. DETAILED DESCRIPTION - The invention also relates to a corresponding authorization arrangement and computer program product.; USE - Authorization of a mobile agent in a communications network, e.g. for use in providing tickets online. ADVANTAGE - A finely granulated system and task specific authorization of agents can be implemented in a simple fashion. DESCRIPTION OF DRAWING(S) - The figure shows authorization of an agent according to the invention. The system shown is for an online ticket server to which agents or users connect for the issuing of a service, in this case a ticket.
PA: (SIEI) SIEMENS AG;
IN: FISCHER K; LOTZ V; WAIDELICH F;
FA: WO2003088012-A1 23.10.2003; AU2003232596-A1 27.10.2003;
DE10215746-A1 06.11.2003;
CO: AE; AG; AL; AM; AT; AU; AZ; BA; BB; BE; BG; BR; BY; BZ; CA;
CH; CN; CO; CR; CU; CY; CZ; DE; DK; DM; DZ; EA; EC; EE; ES; FI;
FR; GB; GD; GE; GH; GM; GR; HR; HU; ID; IE; IL; IN; IS; IT; JP;
KE; KG; KP; KR; KZ; LC; LK; LR; LS; LT; LU; LV; MA; MC; MD; MG;
MK; MN; MW; MX; MZ; NI; NL; NO; NZ; OA; OM; PH; PL; PT; RO; RU;
SC; SD; SE; SG; SI; SK; SL; SZ; TJ; TM; TN; TR; TT; TZ; UA; UG;
US; UZ; VC; VN; WO; YU; ZA; ZM; ZW;
DN: AE; AG; AL; AM; AT; AU; AZ; BA; BB; BG; BR; BY; BZ; CA; CH;
CN; CO; CR; CU; CZ; DK; DM; DZ; EC; EE; ES; FI; GB; GD; GE; GH;
GM; HR; HU; ID; IL; IN; IS; JP; KE; KG; KP; KR; KZ; LC; LK; LR;
LS; LT; LU; LV; MA; MD; MG; MK; MN; MW; MX; MZ; NI; NO; NZ; OM;
PH; PL; PT; RO; RU; SC; SD; SE; SG; SK; SL; TJ; TM; TN; TR; TT;
TZ; UA; UG; US; UZ; VC; VN; YU; ZA; ZM; ZW;
DR: AT; BE; BG; CH; CY; CZ; DE; DK; EA; EE; ES; FI; FR; GB; GH;
GM; GR; HU; IE; IT; KE; LS; LU; MC; MW; MZ; NL; OA; PT; SD; SE;
SI; SK; SL; SZ; TR; TZ; UG; ZM; ZW;
IC: G06F-001/00; H04L-009/32; H04L-012/16; H04L-029/06;
MC: T01-N01A2A; T01-N02B1; T01-S03;
DC: T01;
FN: 2003833818.gif
PR: DE1015746 10.04.2002;
FP: 23.10.2003
UP: 08.06.2004



X

(4)



(19) BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENT- UND
MARKENAMT

Offenlegungsschrift

DE 102 15 746 A 1

(51) Int. Cl.⁷:
H 04 L 9/32
H 04 L 12/16

(21) Aktenzeichen: 102 15 746.4
(22) Anmeldetag: 10. 4. 2002
(43) Offenlegungstag: 6. 11. 2003

DE 102 15 746 A 1

(71) Anmelder:
Siemens AG, 80333 München, DE

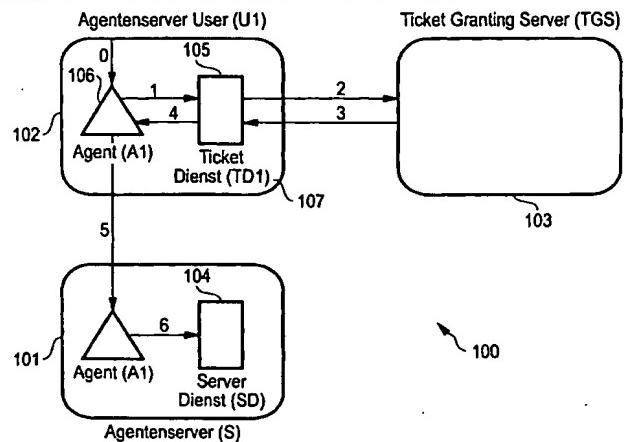
(72) Erfinder:
Fischer, Kai, 81673 München, DE; Lotz, Volkmar,
80639 München, DE; Waidelich, Fabienne, Dr.,
80639 München, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(34) Verfahren und Anordnung sowie Computerprogramm mit Programmcode-Mitteln und Computerprogramm-Produkt zur Autorisierung eines mobilen Agenten in einem Kommunikationsnetz

(57) Die Erfindung betrifft eine Autorisierung eines mobilen Agenten in einem Kommunikationsnetz für einen in dem Kommunikationsnetz angebotenen Dienst. Dabei wird an eine Autorisierungsinstanz in dem Kommunikationsnetz eine Autorisierungsanfrage zur Autorisierung des mobilen Agenten für den Dienst gestellt. Die Autorisierungsanfrage wird von der Autorisierungsinstanz überprüft. Anschließend werden Autorisierungsdaten dann von der Autorisierungsinstanz erzeugt, wenn die Überprüfung eine Berechtigung des mobilen Agenten für den Dienst anzeigen, welche Autorisierungsdaten den mobilen Agenten für den Dienst autorisieren und mit welchen der mobile Agent ausstattbar ist.



DE 102 15 746 A 1

DE 102 15 746 A 1

1

Beschreibung

- [0001] Die Erfindung betrifft eine Autorisierung eines mobilen Agenten in einem Kommunikationsnetz für einen in dem Kommunikationsnetz angebotenen Dienst.
[0002] Mobile Agenten sind aus [1] bekannt.
[0003] Mobile Agenten sind selbstständig agierende Computerprogramme, die autonom, zielgerichtet und arbeitsteilig im Auftrag einer Person oder Organisation (Autorität) Aufträge ausführen. Dabei sind sie autorisiert, in Namen der Autorität Entscheidungen zu treffen.
[0004] Mobile Agenten sind mobil, d. h. sie können während ihrer Lebenszyklen ihre jeweilige Ausführungsumgebung ändern, beispielsweise dadurch, dass sie in Kommunikationsnetzen von einem Kommunikationsgerät zu einem zweiten Kommunikationsgerät migrieren.
[0005] Mobile Agenten werden von Agentenplattformen bzw. in Agentensystemen erzeugt, welche neben der Agentenerzeugung die Agenten interpretieren, ausführen, übertragen und terminieren sowie Verbindungen zwischen Autoritäten und Agenten sowie zwischen Agenten herstellen.
[0006] Ferner werden von Agentenplattformen und/oder in Agentensystemen Dienste für die Autoritäten bzw. für die die Autoritäten vertretenden Agenten angeboten, wie Informationsdienste, elektronische Marktplätze oder elektronische Finanzdienstleistungen.
[0007] Diese Dienste sind einerseits öffentlich zugänglich, d. h. alle Autoritäten können diese Dienste mittels der sie vertretenden Agenten in Anspruch nehmen.
[0008] Andererseits werden auch Dienste angeboten, die nur einer geschlossenen Benutzergruppe, d. h. nur entsprechend berechtigten Autoritäten bzw. deren Agenten, zugänglich sind.
[0009] Für den Zugriff auf solche meist kostenpflichtigen, geschützten Dienste müssen die Agenten als Stellvertreter ihrer Autoritäten autorisiert werden.
[0010] Bei der Autorisierung eines Agenten wird zwischen einer grob granularen und einer fein granularen Autorisierung unterschieden.
[0011] Unter fein granular ist eine Einschränkung der Zugriffsrechte der Agenten auf die Dienste im Hinblick auf z. B. Umfang, Zeitdauer, Zeitpunkt und/oder Funktionalität zu verstehen. Dadurch, dass ein Agent bei der fein granularen Autorisierung nur solche Zugriffsrechte erhält bzw. nur für solche Zugriffsrechte autorisiert wird, welche für die auf ihn übertragene Aufgabe notwendig sind, wird ein möglicher Missbrauch von Agenten für andere Aufgaben eingeschränkt.
[0012] Im Gegensatz dazu erhält ein Agent bei einer grob granularen Autorisierung Zugriffsrechte uneingeschränkt.
[0013] Eine grob granulare Autorisierung ist aus [2], einer Agentenplattform SeMoA[®], bekannt.
[0014] Bei der Agentenplattform SeMoA[®] authentifizieren sich Agenten durch eine eindeutige und nicht manipulierbare ID. Solche IDs sind durch kryptographische Verfahren direkt an die Autoritäten der Agenten gebunden, d. h. ein Agent verfügt über die gesamte Rechtemenge seiner jeweiligen Autorität.
[0015] Aus [3], einer Agentenplattform Ajanta, ist eine fein granulare Autorisierung bekannt.
[0016] Bei der Agentenplattform Ajanta erfolgt die fein granulare Autorisierung eines Agenten durch die entsprechende Autorität des Agenten selbst, was einen sogenannten, zusätzlichen Policy-Abgleich, d. h. eine Überprüfung der Zugriffsrechte unter übergeordneten Gesichtspunkten (Policy), beim Dienstanbieter erfordert.
[0017] Darüber hinaus wird durch diese Vorgehensweise der Autorisierung bei [3] eine Übertragung von Rechten von

2

- einem autorisierten Agenten auf einen anderen Agenten (Delegation) erschwert, weil dabei sogenannte Attributketten, auch bekannt aus [6], welche die Übertragung nachzeichnen, zu bilden sind.
5 [0018] Eine Delegation ermöglicht, Teilaufgaben auch von zweiten Agenten, welche im Auftrag der ursprünglich autorisierten, ersten Agenten handeln, ausführen zu lassen. Diese zweiten Agenten können auch Agenten anderer Autoritäten sein.
10 [0019] Zu berücksichtigende Sicherheitsaspekte bei den mobilen Agenten erfordern außerdem, dass mobile Agenten kein privates bzw. geheimes Schlüsselmaterial mit sich führen dürfen. Sie sind somit nicht in der Lage, auf entfernten Agentenplattformen kryptographische Operationen mit solchen Schlüsseln durchzuführen.
15 [0020] Aus [4] ist eine Autorisierung, ein sogenannter "Kerberos Network Authentication Service", zur Autorisierung eines Client durch einen Server in einer Client/Server-Umgebung bekannt.
20 [0021] Die Autorisierung bei dem "Kerberos Network Authentication Service" erfolgt unter Verwendung von Authentifikations- und Autorisierungsprotokollen und beruht darauf, dass eine kryptographische Operation mit privaten bzw. geheimen Schlüsseln notwendig ist.
25 [0022] Somit liegt der Erfindung die Aufgabe zugrunde, eine fein granulare und aufgabenspezifische Autorisierung eines Agenten auf einfache Weise zu ermöglichen. Darüber hinaus soll die Erfindung es ermöglichen, auf einfache Weise Zugriffsrechte von einem ersten Agenten auf einen zweiten Agenten zu delegieren.
30 [0023] Diese Aufgaben werden durch das Verfahren und die Anordnung sowie durch das Computerprogramm mit Programmcode-Mitteln und das Computerprogramm-Produkt zur Autorisierung eines mobilen Agenten in einem Kommunikationsnetz mit den Merkmalen gemäß dem jeweiligen unabhängigen Patentanspruch gelöst.
35 [0024] Bei dem Verfahren zur Autorisierung eines mobilen Agenten in einem Kommunikationsnetz für einen in dem Kommunikationsnetz angebotenen Dienst werden
40 a) an eine Autorisierungsinstanz in dem Kommunikationsnetz eine Autorisierungsanfrage zur Autorisierung des mobilen Agenten für den Dienst gestellt,
b) die Autorisierungsanfrage von der Autorisierungsinstanz überprüft und
45 c) Autorisierungsdaten dann von der Autorisierungsinstanz erzeugt, wenn die Überprüfung eine Berechtigung des mobilen Agenten für den Dienst anzeigen, welche Autorisierungsdaten den mobilen Agenten für den Dienst autorisieren und mit welchen der mobile Agent ausstattbar ist.
50 [0025] Die Anordnung zur Autorisierung eines mobilen Agenten in einem Kommunikationsnetz für einen in dem Kommunikationsnetz angebotenen Dienst ist derart eingerichtet, dass
55 – an sie eine Autorisierungsanfrage zur Autorisierung des mobilen Agenten für den Dienst stellbar ist,
– durch sie die Autorisierungsanfrage überprüfbar ist und dann, wenn die Überprüfung eine Berechtigung des mobilen Agenten für den Dienst anzeigen, Autorisierungsdaten erzeugbar sind, welche den mobilen Agenten für den Dienst autorisieren und mit welchen der mobile Agent ausstattbar ist.
60 [0026] Das Computerprogramm mit Programmcode-Mitteln ist eingerichtet, um alle Schritte gemäß dem erfindungs-

gemäßen Verfahren durchzuführen, wenn das Programm auf einem Computer ausgeführt wird.

[0027] Das Computerprogramm-Produkt mit auf einem maschinenlesbaren Träger gespeicherten Programmcode-Mitteln ist eingerichtet, um alle Schritte gemäß dem erfindungsgemäßen Verfahren durchzuführen, wenn das Programm auf einem Computer ausgeführt wird.

[0028] Die Anordnung sowie das Computerprogramm mit Programmcode-Mitteln, eingerichtet um alle Schritte gemäß dem erforderlichen Verfahren durchzuführen, wenn das Programm auf einem Computer ausgeführt wird, sowie das Computerprogramm-Produkt mit auf einem maschinenlesbaren Träger gespeicherten Programmcode-Mitteln, eingerichtet um alle Schritte gemäß dem erforderlichen Verfahren durchzuführen, wenn das Programm auf einem Computer ausgeführt wird, sind insbesondere geeignet zur Durchführung des erfindungsgemäßen Verfahrens oder einer seiner nachfolgend erläuterten Weiterbildungen.

[0029] Der Erfindung liegt der Grundgedanke zugrunde, Prinzipien des Client/Server-Umfelds in nicht trivialer Weise in einen Kontext mobiler Agentensysteme zu portieren, diese entsprechend dem neuen Umfeld anzupassen und dabei bei mobilen Agentensystemen vorhandene Mechanismen von Agentenplattformen, wie Authentifikationsverfahren zur eindeutigen und nicht manipulierbaren Authentifikation von mobilen Agenten, in nicht trivialer Weise mit den Prinzipien zu kombinieren und sie zu nutzen.

[0030] Dabei ist ein grundlegender Gedanke der Erfindung, die Autorisierung von Agenten durch sogenannte Autorisierungsdaten zu realisieren. Diese werden bei der Erfindung von einer zentralen Instanz, der Autorisierungsinstanz, ausgestellt und sind auf eindeutige Weise dem jeweiligen Agenten zugeordnet.

[0031] Die Autorisierungsdaten enthalten die Informationen für die fein granulare und aufgabenspezifische Autorisierung, wobei auch übergeordnete, globale Gesichtspunkte, eine sogenannte Policy, zentral berücksichtigt werden kann.

[0032] Gerade dadurch, dass die Autorisierungsdaten von einer zentralen Instanz und eben nicht lokal ausgestellt werden, d. h. von einer Autorität, welche den mobilen Agenten in der Regel erzeugt, können zentral bzw. auf übergeordneter Ebene globale Gesichtspunkte bzw. Randbedingungen (Policy), wie bestimmte globale Einschränkungen von Zugriffsrechten, berücksichtigt werden.

[0033] Agenten erhalten somit bei der Erfindung in Form der jeweiligen Autorisierungsdaten nur diejenigen Rechte, die tatsächlich zur Ausführung der an sie gestellten Aufgabe notwendig sind.

[0034] Durch diesen Ansatz wird die Möglichkeit minimiert, dass ein Agent eine andere als diejenige durchführt, für die er von seiner Autorität instruiert wurde.

[0035] Weiterhin ermöglicht die Erfindung, dass Agenten ihre Rechte oder auch nur eine Teilmenge ihrer Rechte an andere Agenten delegieren können. Rechte können sowohl an Agenten derselben Autorität als auch an Agenten anderer Autoritäten delegiert werden.

[0036] Bevorzugte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

[0037] Die im weiteren beschriebenen Weiterbildungen beziehen sich sowohl auf die Verfahren als auch auf die Anordnung.

[0038] Die Erfindung und die im weiteren beschriebenen Weiterbildungen können sowohl in Software als auch in Hardware, beispielsweise unter Verwendung einer speziellen elektrischen Schaltung, realisiert werden.

[0039] Ferner ist eine Realisierung der Erfindung oder einer im weiteren beschriebenen Weiterbildung möglich durch ein computerlesbares Speichermedium, auf welchem

das Computerprogramm mit Programmcode-Mitteln gesichert ist, welches die Erfindung oder Weiterbildung ausführt.

[0040] Auch kann die Erfindung oder jede im weiteren beschriebene Weiterbildung durch ein Computerprogrammzeugnis realisiert sein, welches ein Speichermedium aufweist, auf welchem das Computerprogramm mit Programmcode-Mitteln gesichert ist, welches die Erfindung oder Weiterbildung ausführt.

[0041] Zur Spezifizierung der Autorisierung des mobilen Agenten ist es zweckmäßig, dass die Autorisierungsdaten mindestens eine der folgenden Informationen enthalten:

- eine Gültigkeitsdauer, wie lange die Autorisierung gültig ist,
- eine Autorisierungsinformation, welche den Dienst kennzeichnet, insbesondere einen Umfang des Dienstes, einen Anbieter des Dienstes, eine Lokalisationsinformation des Anbieters des Dienstes,
- eine Agenteninformation, welche den mobilen Agenten, welcher für den Dienst autorisiert wurde, bezeichnet (Agenten-ID).

[0042] Derartige Autorisierungsdaten ermöglichen eine eindeutige Verknüpfung zwischen klar definierten Zugriffsrechten und dem entsprechend autorisierten mobilen Agenten. Dadurch werden Manipulationsmöglichkeiten eingeschränkt.

[0043] Ferner kann die Sicherheit vor Manipulation und Missbrauch auch dadurch erhöht werden, dass die Autorisierungsanfrage und/oder die Autorisierungsdaten unter Verwendung eines kryptographischen Verfahrens/kryptischer Verfahren, wie eine digitale Signatur, geschützt werden. Verwendbare kryptographische Verfahren sind in [5] beschrieben.

[0044] Des weiteren ist es sinnvoll, eine Kommunikation bzw. einen Datenaustausch zwischen der Autorisierungsinstanz und dem mobilen Agenten durch einen Ticketdienst abzuwickeln. Dadurch lassen sich einzelne klar strukturierte, funktionelle Module bzw. Komponenten, beispielsweise durch entsprechend eingerichtete Server, realisieren.

[0045] So wäre dementsprechend die Funktion eines solchen Ticketdienstes das Stellen der Anfrage an die Autorisierungsinstanz, das Empfangen und Weiterreichen der Autorisierungsdaten an den mobilen Agenten. Auch zusätzliche Aufgaben bei Agentenplattformen und/oder Agentensystemen kann ein solcher Ticketdienst übernehmen, wie eine Authentifikationsprüfung des mobilen Agenten und/oder eine Authentifikationsprüfung der Autorisierungsinstanz.

[0046] Auch ist es möglich, den Ticketdienst und die Autorisierungsinstanz in einer Instanz zu integrieren.

[0047] Auch ist es sinnvoll, die Autorisierungsdaten in einem Ticket zusammenzufassen. Grundzüge einer Tickettechnik sind aus [4] bekannt.

[0048] Das Ticket kann durch kryptographische Verfahren [5] vor Missbrauch und Manipulationen geschützt werden. Eine Verknüpfung des auf einen mobilen Agenten ausgestellten Tickets mit diesem wird durch die Authentifikation des mobilen Agenten gewährleistet.

[0049] Ist nun der mobile Agent mit dem Ticket ausgestattet, so migriert er innerhalb des Kommunikationsnetzes, dorthin, wo der von ihm nachzufragende Dienst, beispielsweise ein Reisedienst oder ein Einkaufsdienst, bzw. der entsprechende Dienstanbieter lokalisiert ist. Dort wird der mobile Agent authentifiziert. Beim Versuch des Zugriffs auf den Dienst muss der mobile Agent seine Legitimation beweisen, was durch Übergabe des Tickets an den Dienstanbieter und die Überprüfung des Tickets und der dort nieder-

gelegten Berechtigung durch den Dienstanbieter erfolgt.
[0050] In einem solchen Rechnernetz sind in der Regel der Dienstanbieter, die Autorisierungsinstantz sowie der Ticketdienst durch Server realisiert.

[0051] Ein mobile Agent selbst wird in der Regel dann erzeugt, wenn ein Kommunikationsteilnehmer in dem Kommunikationsnetz einen dort angebotenen Dienst in Anspruch nehmen möchte.

[0052] In einer Weiterbildung stellt der mobile Agent die Autorisierungsanfrage für sich selbst, d. h. er selbst möchte auf ihn ausgestellte und ihn autorisierende Autorisierungsdaten haben.

[0053] Alternativ ist es auch möglich, dass ein anderer, zweiter autorisierter mobiler Agent die Autorisierungsanfrage für den ersten mobilen Agenten stellt. Die Autorisierungsdaten werden dann auf Basis der Autorisierung des anderen, zweiten mobilen Agenten für den ersten mobilen Agenten ausgestellt. Der erste mobile Agent erhält anschließend direkt oder indirekt von dem anderen, zweiten mobilen Agenten die auf ihn ausgestellten Autorisierungsdaten.

[0054] Diese Vorgehensweise eignet sich insbesondere zu einer Übertragung von Autorisierungen, was als Delegation bezeichnet wird.

[0055] In diesem Fall wäre bei obiger Vorgehensweise der andere, zweite mobile Agent ein sogenannter Delegationsagent. Er delegiert seine ursprüngliche Autorisierung, d. h. seine ursprünglichen Rechte, an den ersten mobilen Agenten.

[0056] Im Detail kann eine solche Delegation derart realisiert werden:

- der Delegationsagent ist durch ursprüngliche Autorisierungsdaten ursprünglich für den Dienst autorisiert,
- der Delegationsagent stellt die Autorisierungsanfrage für den mobilen Agenten, durch welche die Autorisierungsdaten für den mobilen Agenten unter Verwendung der ursprünglichen Autorisierungsdaten erzeugt werden,
- der mobile Agent wird mit den Autorisierungsdaten ausgestattet, wobei die ursprünglichen Autorisierung des Delegationsagenten auf den mobilen Agenten übertragen wird.

[0057] In Figuren sind Ausführungsbeispiele der Erfahrung dargestellt, welche im weiteren näher erläutert werden.

[0058] Es zeigen

[0059] Fig. 1 Autorisierung eines mobilen Agenten gemäß einem ersten Ausführungsbeispiel;

[0060] Fig. 2 Autorisierung eines zweiten mobilen Agenten durch Übertragung einer Autorisierung von einem ersten autorisierten Agenten auf den zweiten mobilen Agenten gemäß einem zweiten Ausführungsbeispiel.

[0061] Erstes Ausführungsbeispiel: Autorisierung eines mobilen Agenten in einem Agentensystem In Fig. 1 ist ein Ausschnitt eines Rechnernetzes 100 mit mehreren miteinander vernetzten Servern 101, 102, 103, auf welchen ein Agentensystem mit entsprechend eingerichteten Agentenplattformen implementiert ist, dargestellt.

[0062] Grundlegende Netz- und Servertechniken sowie Agentenplattformen sind allgemein bekannt.

[0063] Fig. 1 zeigt einen Server 101 eines Dienstanbieters S (Agentenserver S 101), welcher einen zugangsbeschränkten und kostenpflichtigen Dienst SD 104, in diesem Fall einen Reisebuchungsdienst, anbietet.

[0064] Fig. 1 zeigt ferner einen Server 102 (Agentenserver User U1 102) eines Benutzers U1 (User U1). Auf dem Agentenserver User U1 102 ist ein Ticket Dienst (TD1) 107, ein entsprechend programmiertes Computerprogramm, im-

plementiert, mittels welchem Zugriffsrechte in Form von so genannten Tickets 105 auf Dienste in dem Rechnernetz 100 erlangbar sind.

[0065] Auch zeigt Fig. 1 einen Ticket Granting Server 103, welcher Autorisierungszertifikate, die sogenannten Tickets 105, für mobile Agenten des Agentensystems, wie Agent A1 106, ausstellt.

[0066] Grundzüge einer Tickettechnik sind in [4] beschrieben.

5 10 [0067] Ein von dem Ticket Granting Server 103 ausgestelltes Ticket 105 ist auf eindeutige Weise demjenigen Agenten, beispielsweise dem Agenten A1 106, zugeordnet, für den es ausgestellt wird. Es definiert das dem Agenten zu

15 gestandene Recht. Dazu enthält das Ticket 105 entsprechende Autorisierungsdaten. Die Autorisierungsdaten setzen sich zusammen aus einer Agenten ID, einer Gültigkeitsdauer des Tickets 105, einer Angabe, wo und wie es einzulösen ist, sowie aus einer Beschreibung des konkreten zugestandene Rechts.

20 [0068] Das Ticket 105 ist darüber hinaus durch eine digitale Signatur vor Missbrauch und Manipulationen geschützt.

[0069] In Fig. 1 dargestellte Pfeile 0 bis 6 kennzeichnen die bei einer Nachfrage nach dem Dienstes SD 104 ablaufenden Schritte 0 bis 6.

25 30 35 40 45 50 55 60 65 70 75 80 85 90 95 100 105 110 115 120 125 130 135 140 145 150 155 160 165 170 175 180 185 190 195 200 205 210 215 220 225 230 235 240 245 250 255 260 265 270 275 280 285 290 295 300 305 310 315 320 325 330 335 340 345 350 355 360 365 370 375 380 385 390 395 400 405 410 415 420 425 430 435 440 445 450 455 460 465 470 475 480 485 490 495 500 505 510 515 520 525 530 535 540 545 550 555 560 565 570 575 580 585 590 595 600 605 610 615 620 625 630 635 640 645 650 655 660 665 670 675 680 685 690 695 700 705 710 715 720 725 730 735 740 745 750 755 760 765 770 775 780 785 790 795 800 805 810 815 820 825 830 835 840 845 850 855 860 865 870 875 880 885 890 895 900 905 910 915 920 925 930 935 940 945 950 955 960 965 970 975 980 985 990 995 1000 1005 1010 1015 1020 1025 1030 1035 1040 1045 1050 1055 1060 1065 1070 1075 1080 1085 1090 1095 1100 1105 1110 1115 1120 1125 1130 1135 1140 1145 1150 1155 1160 1165 1170 1175 1180 1185 1190 1195 1200 1205 1210 1215 1220 1225 1230 1235 1240 1245 1250 1255 1260 1265 1270 1275 1280 1285 1290 1295 1300 1305 1310 1315 1320 1325 1330 1335 1340 1345 1350 1355 1360 1365 1370 1375 1380 1385 1390 1395 1400 1405 1410 1415 1420 1425 1430 1435 1440 1445 1450 1455 1460 1465 1470 1475 1480 1485 1490 1495 1500 1505 1510 1515 1520 1525 1530 1535 1540 1545 1550 1555 1560 1565 1570 1575 1580 1585 1590 1595 1600 1605 1610 1615 1620 1625 1630 1635 1640 1645 1650 1655 1660 1665 1670 1675 1680 1685 1690 1695 1700 1705 1710 1715 1720 1725 1730 1735 1740 1745 1750 1755 1760 1765 1770 1775 1780 1785 1790 1795 1800 1805 1810 1815 1820 1825 1830 1835 1840 1845 1850 1855 1860 1865 1870 1875 1880 1885 1890 1895 1900 1905 1910 1915 1920 1925 1930 1935 1940 1945 1950 1955 1960 1965 1970 1975 1980 1985 1990 1995 2000 2005 2010 2015 2020 2025 2030 2035 2040 2045 2050 2055 2060 2065 2070 2075 2080 2085 2090 2095 2100 2105 2110 2115 2120 2125 2130 2135 2140 2145 2150 2155 2160 2165 2170 2175 2180 2185 2190 2195 2200 2205 2210 2215 2220 2225 2230 2235 2240 2245 2250 2255 2260 2265 2270 2275 2280 2285 2290 2295 2300 2305 2310 2315 2320 2325 2330 2335 2340 2345 2350 2355 2360 2365 2370 2375 2380 2385 2390 2395 2400 2405 2410 2415 2420 2425 2430 2435 2440 2445 2450 2455 2460 2465 2470 2475 2480 2485 2490 2495 2500 2505 2510 2515 2520 2525 2530 2535 2540 2545 2550 2555 2560 2565 2570 2575 2580 2585 2590 2595 2600 2605 2610 2615 2620 2625 2630 2635 2640 2645 2650 2655 2660 2665 2670 2675 2680 2685 2690 2695 2700 2705 2710 2715 2720 2725 2730 2735 2740 2745 2750 2755 2760 2765 2770 2775 2780 2785 2790 2795 2800 2805 2810 2815 2820 2825 2830 2835 2840 2845 2850 2855 2860 2865 2870 2875 2880 2885 2890 2895 2900 2905 2910 2915 2920 2925 2930 2935 2940 2945 2950 2955 2960 2965 2970 2975 2980 2985 2990 2995 3000 3005 3010 3015 3020 3025 3030 3035 3040 3045 3050 3055 3060 3065 3070 3075 3080 3085 3090 3095 3100 3105 3110 3115 3120 3125 3130 3135 3140 3145 3150 3155 3160 3165 3170 3175 3180 3185 3190 3195 3200 3205 3210 3215 3220 3225 3230 3235 3240 3245 3250 3255 3260 3265 3270 3275 3280 3285 3290 3295 3300 3305 3310 3315 3320 3325 3330 3335 3340 3345 3350 3355 3360 3365 3370 3375 3380 3385 3390 3395 3400 3405 3410 3415 3420 3425 3430 3435 3440 3445 3450 3455 3460 3465 3470 3475 3480 3485 3490 3495 3500 3505 3510 3515 3520 3525 3530 3535 3540 3545 3550 3555 3560 3565 3570 3575 3580 3585 3590 3595 3600 3605 3610 3615 3620 3625 3630 3635 3640 3645 3650 3655 3660 3665 3670 3675 3680 3685 3690 3695 3700 3705 3710 3715 3720 3725 3730 3735 3740 3745 3750 3755 3760 3765 3770 3775 3780 3785 3790 3795 3800 3805 3810 3815 3820 3825 3830 3835 3840 3845 3850 3855 3860 3865 3870 3875 3880 3885 3890 3895 3900 3905 3910 3915 3920 3925 3930 3935 3940 3945 3950 3955 3960 3965 3970 3975 3980 3985 3990 3995 4000 4005 4010 4015 4020 4025 4030 4035 4040 4045 4050 4055 4060 4065 4070 4075 4080 4085 4090 4095 4100 4105 4110 4115 4120 4125 4130 4135 4140 4145 4150 4155 4160 4165 4170 4175 4180 4185 4190 4195 4200 4205 4210 4215 4220 4225 4230 4235 4240 4245 4250 4255 4260 4265 4270 4275 4280 4285 4290 4295 4300 4305 4310 4315 4320 4325 4330 4335 4340 4345 4350 4355 4360 4365 4370 4375 4380 4385 4390 4395 4400 4405 4410 4415 4420 4425 4430 4435 4440 4445 4450 4455 4460 4465 4470 4475 4480 4485 4490 4495 4500 4505 4510 4515 4520 4525 4530 4535 4540 4545 4550 4555 4560 4565 4570 4575 4580 4585 4590 4595 4600 4605 4610 4615 4620 4625 4630 4635 4640 4645 4650 4655 4660 4665 4670 4675 4680 4685 4690 4695 4700 4705 4710 4715 4720 4725 4730 4735 4740 4745 4750 4755 4760 4765 4770 4775 4780 4785 4790 4795 4800 4805 4810 4815 4820 4825 4830 4835 4840 4845 4850 4855 4860 4865 4870 4875 4880 4885 4890 4895 4900 4905 4910 4915 4920 4925 4930 4935 4940 4945 4950 4955 4960 4965 4970 4975 4980 4985 4990 4995 5000 5005 5010 5015 5020 5025 5030 5035 5040 5045 5050 5055 5060 5065 5070 5075 5080 5085 5090 5095 5100 5105 5110 5115 5120 5125 5130 5135 5140 5145 5150 5155 5160 5165 5170 5175 5180 5185 5190 5195 5200 5205 5210 5215 5220 5225 5230 5235 5240 5245 5250 5255 5260 5265 5270 5275 5280 5285 5290 5295 5300 5305 5310 5315 5320 5325 5330 5335 5340 5345 5350 5355 5360 5365 5370 5375 5380 5385 5390 5395 5400 5405 5410 5415 5420 5425 5430 5435 5440 5445 5450 5455 5460 5465 5470 5475 5480 5485 5490 5495 5500 5505 5510 5515 5520 5525 5530 5535 5540 5545 5550 5555 5560 5565 5570 5575 5580 5585 5590 5595 5600 5605 5610 5615 5620 5625 5630 5635 5640 5645 5650 5655 5660 5665 5670 5675 5680 5685 5690 5695 5700 5705 5710 5715 5720 5725 5730 5735 5740 5745 5750 5755 5760 5765 5770 5775 5780 5785 5790 5795 5800 5805 5810 5815 5820 5825 5830 5835 5840 5845 5850 5855 5860 5865 5870 5875 5880 5885 5890 5895 5900 5905 5910 5915 5920 5925 5930 5935 5940 5945 5950 5955 5960 5965 5970 5975 5980 5985 5990 5995 6000 6005 6010 6015 6020 6025 6030 6035 6040 6045 6050 6055 6060 6065 6070 6075 6080 6085 6090 6095 6100 6105 6110 6115 6120 6125 6130 6135 6140 6145 6150 6155 6160 6165 6170 6175 6180 6185 6190 6195 6200 6205 6210 6215 6220 6225 6230 6235 6240 6245 6250 6255 6260 6265 6270 6275 6280 6285 6290 6295 6300 6305 6310 6315 6320 6325 6330 6335 6340 6345 6350 6355 6360 6365 6370 6375 6380 6385 6390 6395 6400 6405 6410 6415 6420 6425 6430 6435 6440 6445 6450 6455 6460 6465 6470 6475 6480 6485 6490 6495 6500 6505 6510 6515 6520 6525 6530 6535 6540 6545 6550 6555 6560 6565 6570 6575 6580 6585 6590 6595 6600 6605 6610 6615 6620 6625 6630 6635 6640 6645 6650 6655 6660 6665 6670 6675 6680 6685 6690 6695 6700 6705 6710 6715 6720 6725 6730 6735 6740 6745 6750 6755 6760 6765 6770 6775 6780 6785 6790 6795 6800 6805 6810 6815 6820 6825 6830 6835 6840 6845 6850 6855 6860 6865 6870 6875 6880 6885 6890 6895 6900 6905 6910 6915 6920 6925 6930 6935 6940 6945 6950 6955 6960 6965 6970 6975 6980 6985 6990 6995 7000 7005 7010 7015 7020 7025 7030 7035 7040 7045 7050 7055 7060 7065 7070 7075 7080 7085 7090 7095 7100 7105 7110 7115 7120 7125 7130 7135 7140 7145 7150 7155 7160 7165 7170 7175 7180 7185 7190 7195 7200 7205 7210 7215 7220 7225 7230 7235 7240 7245 7250 7255 7260 7265 7270 7275 7280 7285 7290 7295 7300 7305 7310 7315 7320 7325 7330 7335 7340 7345 7350 7355 7360 7365 7370 7375 7380 7385 7390 7395 7400 7405 7410 7415 7420 7425 7430 7435 7440 7445 7450 7455 7460 7465 7470 7475 7480 7485 7490 7495 7500 7505 7510 7515 7520 7525 7530 7535 7540 7545 7550 7555 7560 7565 7570 7575 7580 7585 7590 7595 7600 7605 7610 7615 7620 7625 7630 7635 7640 7645 7650 7655 7660 7665 7670 7675 7680 7685 7690 7695 7700 7705 7710 7715 7720 7725 7730 7735 7740 7745 7750 7755 7760 7765 7770 7775 7780 7785 7790 7795 7800 7805 7810 7815 7820 7825 7830 7835 7840 7845 7850 7855 7860 7865 7870 7875 7880 7885 7890 7895 7900 7905 7910 7915 7920 7925 7930 7935 7940 7945 7950 7955 7960 7965 7970 7975 7980 7985 7990 7995 8000 8005 8010 8015 8020 8025 8030 8035 8040 8045 8050 8055 8060 8065 8070 8075 8080 8085 8090 8095 8100 8105 8110 8115 8120 8125 8130 8135 8140 8145 8150 8155 8160 8165 8170 8175 8180 8185 8190 8195 8200 8205 8210 8215 8220 8225 8230 8235 8240 8245 8250 8255 8260 8265 8270 8275 8280 8285 8290 8295 8300 8305 8310 8315 8320 8325 8330 8335 8340 8345 8350 8355 8360 8365 8370 8375 8380 8385 8390 8395 8400 8405 8410 8415 8420 8425 8430 8435 8440 8445 8450 8455 8460 8465 8470 8475 8480 8485 8490 8495 8500 8505 8510 8515 8520 8525 8530 8535 8540 8545 8550 8555 8560 8565 8570 8575 8580 8585 8590 8595 8600 8605 8610 8615 8620 8625 8630 8635 8640 8645 8650 8655 8660 8665 8670 8675 8680 8685 8690 8695 8700 8705 8710 8715 8720 8725 8730 8735 8740 8745 8750 8755 8760 8765 8770 8775 8780 8785 8790 8795 8800 8805 8810 8815 8820 8825 8830 8835 8840 8845 8850 8855 8860 8865 8870 8875 8880 8885 8890 8895 8900 8905 8910 8915 8920 8925 8930 8935 8940 8945 8950 8955 8960 8965 8970 8975 8980 8985 8990 8995 9000 9005 9010 9015 9020 9025 9030 9035 9040 9045 9050 9055 9060 9065 9070 9075 9080 9085 9090 9095 9100 9105 9110 9115 9120 9125 9130 9135 9140 9145 9150 9155 9160 9165 9170 9175 9180 9185 9190 9195 9200 9205 9210 9215 9220 9225 9230 9235 9240 9245 9250 9255 9260 9265 9270 9275 9280 9285 9290 9295 9300 9305 9310 9315 9320 9325 9330 9335 9340 9345 9350 9355 9360 9365 9370 9375 9380 9385 9390

6. Der Agent A1 106 möchte auf den Dienst SD 104 zugreifen und übergibt das Ticket 105. Der Dienst SD 104 überprüft die Gültigkeit des Tickets 105 und führt den Zugriff gemäß den im Ticket 105 gespeicherten Rechten aus.

[0070] Zweites Ausführungsbeispiel: Autorisierung eines mobilen Agenten A2 durch Delegation durch den mobilen Agenten A1 106 in dem Agentensystem (Fig. 2)

[0071] Das zweite Ausführungsbeispiel beschreibt zusammen mit Fig. 2 eine Delegation eines zweiten mobilen Agenten A2 201 durch den mobilen Agenten A1 106.

[0072] Ohne Beschränkung der Allgemeinheit ist der zweite Agent A2 201 einem anderen Benutzer als User U1 zugehörig.

[0073] Die in Fig. 2 dargestellten Pfeile 1 bis 8 kennzeichnen die bei der Delegation (der Nachfrage nach dem Dienstes SD 104) ablaufenden Schritte 1 bis 8.

[0074] Ausgangssituation bei der nachfolgend beschrieben Delegation ist, dass der Agent A1 106 im Besitz des auf ihn ausgestellten Tickets 105 ist. Des weiteren befindet sich der Agent A1 106 auf der Agentenplattform des Agenten-servers S 101. Auf dieses befindet sich ebenfalls der Agent A2 201.

1. Agent A1 106 migriert zum Agentenserver User U1 102. Beim Betreten der Agentenplattform wird der Agent A1 106 eindeutig und nicht manipulierbar authentifiziert.

2. Der Agent A1 106 fordert beim Ticket-Dienst TD1 107 ein Ticket (T2) 202 für den Agenten A2 201 an. Der Ticket-Dienst TD1 107 ermittelt die eindeutige Identität vom Agenten A1 106.

3. Der Ticket-Dienst TDI 107 fordert bei dem Ticket-Granting-Server (TGS) 103 das Ticket 202 für den Agenten A2 201 an (Ticket Request).

Hierfür wird dem Ticket Granting Server TGS 103 die eindeutige Identität von Agent A1 106 und von Agent A2 201 mitgeteilt. Auch die Authentizität des Users U1 wird wieder überprüft.

Der Ticket Granting Server TGS 103 prüft dann in analoger Weise wie zuvor beim Agenten A1 106, welche Rechte dem Agenten A2 202 zugestanden werden können.

Das Ticket 105 von Agent A1 106 wird als Basis für das Ticket 202 von Agent A2 201 herangezogen.

Der Ticket-Request ist durch kryptographische Operationen geschützt.

4. Der Ticket Granting Server TGS 103 übergibt das für den Agenten A2 201 ausgestellte Ticket 202 an den Ticket Dienst TDI 107 (Ticket Reply).

Der Ticket-Reply ist ebenfalls durch kryptographische Operationen geschützt. Auch die Authentizität des Ticket Granting Servers TGS 103 wird überprüft.

5. Der Agent A1 106 bekommt vom Ticket-Dienst TDI 107 das Ticket 202.

6. Der Agent A1 106 migriert zum Agentenserver S 101. Beim Betreten der Agentenplattform des Agenten-servers S 101 wird der Agent A1 106 eindeutig und nicht manipulierbar authentifiziert.

7. Der Agent A1 106 übergibt das Ticket 201 an den Agenten A2 201.

8. Der Agent A2 201 greift auf den Dienst SD 104 zu und übergibt das Ticket 202. Der Dienst SD 104 überprüft die Gültigkeit des Tickets 202 und führt den Zugriff gemäß den im Ticket 202 gespeicherten Rechten aus.

[0075] In diesem Dokument sind folgende Schriften zitiert:

[1] M. N. Huhns, M. P. Singh; Readings in Agents; Morgan Kaufmann Publishers Inc., 1998;

[2] Agentenplattform SeMoA[®], erhältlich am 23.03.2002 unter: <http://www.semoa.org>

[3] Agentenplattform Ajanta, in "Delegation of Privileges to Mobile Agents in Ajanta", erhältlich am 23.03.2002 unter: <http://www.cs.umn.edu/Ajanta/papers/ic2000.pdf>;

[4] Kerberos (IETF RFC 1510);

[5] Bruce Schneider; Applied Cryptography; Second Edition; John Wiley & Sons, Inc.;

[6] SPKI-Attributzertifikate (IETF RFC2692, IETF RFC2693).

15

Patentansprüche

1. Verfahren zur Autorisierung eines mobilen Agenten in einem Kommunikationsnetz für einen in dem Kommunikationsnetz angebotenen Dienst, bei dem

a) an eine Autorisierungsinstanz in dem Kommunikationsnetz eine Autorisierungsanfrage zur Autorisierung des mobilen Agenten für den Dienst gestellt wird,

b) die Autorisierungsinstanz die Autorisierungsanfrage überprüft und

c) die Autorisierungsinstanz, wenn die Überprüfung eine Berechtigung des mobilen Agenten für den Dienst (bzw. mindestens eines Teils des Dienstes) anzeigt, Autorisierungsdaten erzeugt, welche den mobilen Agenten für den Dienst autorisieren und mit welchen der mobile Agent ausstattbar ist, andernfalls die Autorisierungsinstanz keine Autorisierungsdaten erzeugt.

2. Verfahren nach Anspruch 1, bei dem die Autorisierungsdaten mindestens eine der folgenden Informationen enthalten:

– eine Gültigkeitsdauer, wie lange die Autorisierung gültig ist,

– eine Autorisierungsinformation, welche den Dienst kennzeichnet, insbesondere einen Umfang des Dienstes, einen Anbieter des Dienstes, eine Lokalisierungsinformation des Anbieters des Dienstes,

– eine Agenteninformation, welche den mobilen Agenten, welcher für den Dienst autorisiert wurde, bezeichnet (Agenten-ID).

3. Verfahren nach Anspruch 1 oder 2, bei dem die Autorisierungsanfrage und/oder die Autorisierungsdaten unter Verwendung eines kryptographischen Verfahrens/kryptischer Verfahren geschützt werden.

4. Verfahren nach Anspruch 3, bei dem die Autorisierungsdaten mit einer digitalen Signatur versehen werden.

5. Verfahren nach einem der vorangehenden Ansprüche, bei dem die Autorisierungsanfrage von einem Ticketdienst bei der Autorisierungsinstanz gestellt wird, welcher Ticketdienst den mobilen Agenten mit einem Ticket, welches die Autorisierungsdaten enthält, ausstattet.

6. Verfahren nach einem der vorangehenden Ansprüche, bei dem der Agent unter Verwendung der Autorisierungsdaten bei einem Dienstanbieter um den Dienst nachfragt.

7. Verfahren nach einem der vorangehenden Ansprüche, bei dem das Kommunikationsnetz ein verteiltes Rechnernetz ist, wobei die Autorisierungsinstanz ein Serverrechner in dem verteilten Rechnernetz ist.

60

65

8. Verfahren nach einem der vorgehenden Ansprüchen, bei dem ein Kommunikationsteilnehmer in dem Kommunikationsnetz den Dienst in Anspruch nehmen möchte und dabei den mobilen Agenten erzeugt.
9. Verfahren nach einem der vorgehenden Ansprüche, bei dem der mobile Agent die Autorisierungsanfrage stellt.
10. Verfahren nach einem der Ansprüche 1 bis 8, bei dem ein Delegationsagent die Autorisierungsanfrage für den mobilen Agenten stellt.
11. Verfahren nach Anspruch 10, eingesetzt zur Übertragung einer ursprünglichen Autorisierung des Delegationsagenten für den Dienst auf den mobilen Agenten,
wobei der Delegationsagent durch ursprüngliche Autorisierungsdaten ursprünglich für den Dienst autorisiert war,
wobei der Delegationsagent die Autorisierungsanfrage für den mobilen Agenten stellt, durch welche die Autorisierungsdaten für den mobilen Agenten unter Verwendung der ursprünglichen Autorisierungsdaten erzeugt werden
und wobei der mobile Agent mit den Autorisierungsdaten ausgestattet wird, wobei die ursprünglichen Autorisierung des Delegationsagenten auf den mobilen Agenten übertragen wird.
12. Anordnung zur Autorisierung eines mobilen Agenten in einem Kommunikationsnetz für einen in dem Kommunikationsnetz angebotenen Dienst, an welche Autorisierungsanordnung eine Autorisierungsanfrage zur Autorisierung des mobilen Agenten für den Dienst stellbar ist,
durch welche Autorisierungsanordnung die Autorisierungsanfrage überprüfbar ist und, wenn die Überprüfung eine Berechtigung des mobilen Agenten für den Dienst (bzw. mindestens eines Teils des Dienstes) anzeigen, Autorisierungsdaten erzeugbar sind, welche den mobilen Agenten für den Dienst autorisieren und mit welchen der mobile Agent ausstattbar ist, andernfalls keine Autorisierungsdaten erzeugbar sind.
13. Autorisierungsanordnung nach Anspruch 12, eingesetzt in einem Kommunikationsnetz zur Autorisierung des mobilen Agenten in einem Kommunikationsnetz für den in dem Kommunikationsnetz angebotenen Dienst.
14. Computerprogramm mit Programmcode-Mitteln, um alle Schritte gemäß Anspruch 1 durchzuführen, wenn das Programm auf einem Computer ausgeführt wird.
15. Computerprogramm mit Programmcode-Mitteln gemäß Anspruch 14, die auf einem computerlesbaren Datenträger gespeichert sind.
16. Computerprogramm-Produkt mit auf einem maschinenlesbaren Träger gespeicherten Programmcode-Mitteln, um alle Schritte gemäß Anspruch 1 durchzuführen, wenn das Programm auf einem Computer ausgeführt wird.

Hierzu 2 Seite(n) Zeichnungen

FIG 1

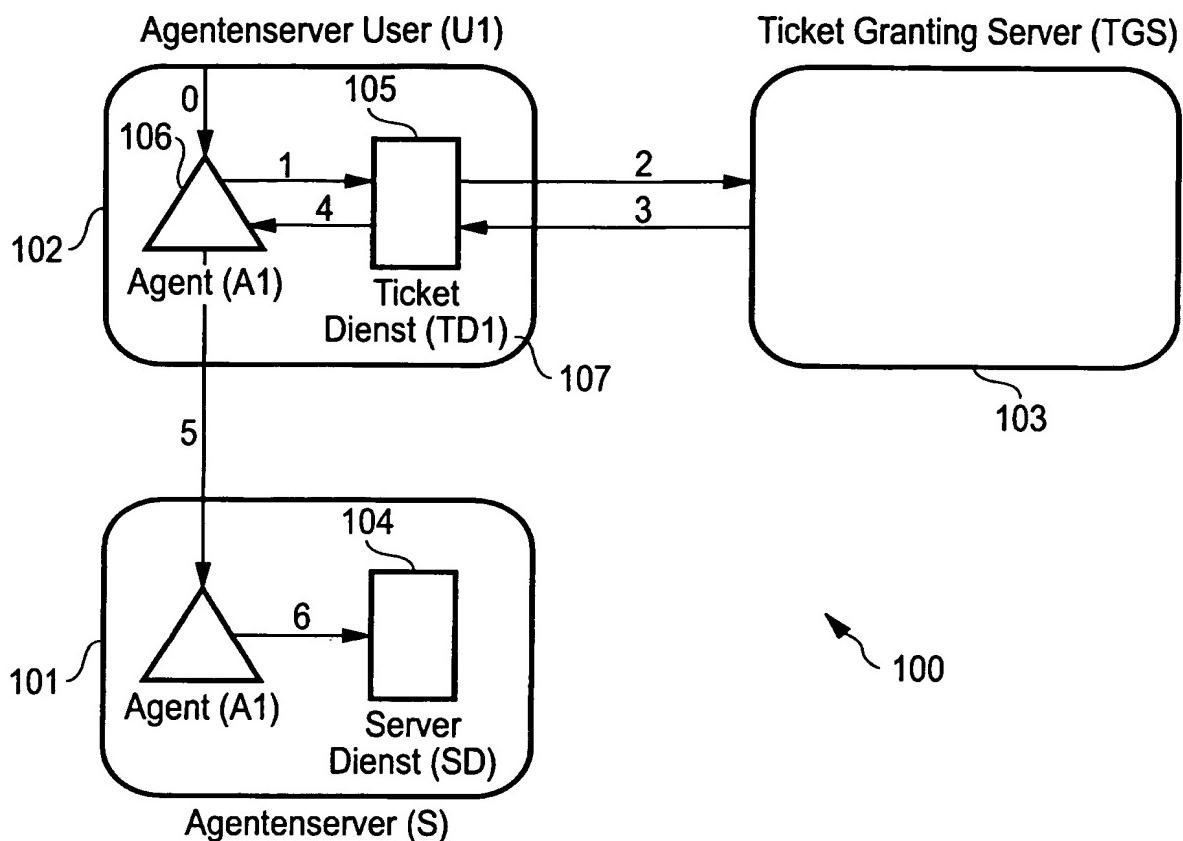


FIG 2